REMARKS

Claims 1, 4, 5, 7-11, 13-16, 18, 21, 23, and 24 are all the claims pending in the application. By this Amendment, Applicant amends claims 1, 18, and 21 to further clarify the features in these claims. Accordingly, Applicant amends claim 7 for conformity therewith and cancels claims 6, 17, and 22.

Incomplete Office Action

Applicant respectfully submits that the Office Action fails to "rebut" Applicant's arguments presented in the Amendment under 37 C.F.R. § 1.111 filed on October 20, 2005. MPEP § 706.07 recites that:

> [i]n making the final rejection, all outstanding grounds of rejection of record should be carefully reviewed, and any such grounds relied on in the final rejection should be reiterated. They must also be clearly developed to such an extent that applicant may readily judge the advisability of an appeal unless a single previous Office action contains a complete statement supporting the rejection. **However, where a single previous Office action contains a complete statement of a ground of rejection, the final rejection may refer to such a statement and also should include a rebuttal of any arguments raised in the applicant's reply,** emphasis added...

The Examiner found a new reference for one of the unique features of independent claim 1. However, arguments presented in the Amendment under 37 C.F.R. § 1.111 filed on October 20, 2005 were directed to other features of claim 1 and are not addressed by the Examiner in the Office Action.

Prior Art Rejection

Of the pending claims, claims 1, 4, 5, 7-11, 13-16, 18, 21, 23, and 24 presently stand rejected. Specifically, these claims are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,564,070 to Want et al. (hereinafter "Want") in view of U.S. Patent No. 5,537,102 to Pinnow (hereinafter "Pinnow"). Applicant respectfully traverses this rejection in view of the following comments.

An aspect of the present invention is to protect access to personal computer applications of a computer station connected to an inter-computer communication network, for example a personalized e-mail or a financial account or other personalized applications. Normally this access to personal applications is automatic when a personal portable object is near to a read unit connected to the station. This object can be preferably a wristwatch, or a bracelet, necklace, ring, card or badge.

To this end, in the method of claim 1, the identification code specific to the portable object, *i.e.* the readable word of a memory of the electronic circuit of the object, has to be searched after transmission to a determined remote server in a checking file of said server. Said "server" is, for example, the watch manufacturer's server that is remote from the computer station with the read unit connected to said computer station. If the readable word has been found in the checking file located on the remote server, a password is sent from the checking file of the remote server to the portable object. Specifically, the password is sent to a control logic module of the electronic circuit of the portable object, which shapes the password for opening a read and/or write barrier of the storage means in which access words are kept secret by said read and/or write barrier. Accordingly, if no password is transmitted from the dedicated server to the

storage means, access words are kept secret, which guarantees the security of the personal information stored in the portable object.

In other words, there are two checking operations to allow for opening the read and/or write barrier of the storage means. First, the readable verification word of the portable object is checked in a file of the server remote from the computer station before sending a password. Second, the password is checked in the control logic module for opening the read and/or write barrier of the storage means. Furthermore, the peripheral read unit is connected to the computer station to give the instruction to the computer station to connect automatically to the remote server, by having the read unit contain the address of the determined remote server in a storage module and an address initiation software.

This method allows, in the event of loss or theft of the portable object, to inactivate the object by ending its validity via any communication means related to the determined server. Accordingly, personal computer applications can not be opened by a lost or stolen object.

The prior art of record fails to disclose or suggest the unique features of the independent claim 1. Independent claim 1 recites:

> a) placing the portable object within the determined detection zone of the read unit so that the peripheral read unit, which includes an antenna of said second signal transmission and reception means, and a printed circuit with all electronic components for controlling said antenna, detects its presence, and reads via the first and second signal transmission and reception means the readable verification word of the memory of the electronic circuit,
>
> b) giving the instruction from the peripheral read unit, which contains the address of the determined server in the storage module, as well as address initiation software, to the computer station to connect itself automatically to the

> communication network for sending the readable verification word toward a checking file of a determined remote server in the communication network,
>
> c) searching in the checking file of the determined remote server to see whether the readable verification word is included in a list of authorized words,
>
> d) only if the readable verification word has been found in the list, sending from the checking file of the determined remote server a password towards the computer station and the read unit, and via the first and second transmission and reception means to a control logic module of the electronic circuit of the portable object, which shapes said password for opening a read and/or write barrier of storage means, which are contained into the memory of said personalized electronic circuit, in which access words to computer applications are kept secret by the read and/or write barrier, and
>
> e) communicating via said first and second transmission and reception means the access words contained in the storage means of the electronic circuit memory of the portable object to the computer station in order to authorize said computer applications to be opened.

Want, on the other hand, discloses a method and a system for maintaining processing continuity to mobile computers in a wireless network. To maintain this processing continuity, portable Tabs, such as PDA (active badges) are used. These portable Tabs include signal transmission and reception means for wireless communication with read units (radio or IR) connected to computer stations in different rooms. This system is a ubiquitous computing environment, where these computers with Tabs work interactively with each other (col. 2, lines 16-20).

The personal Tab includes a display in order to indicate the location of the Tab with its wearer in the environment. The Tab also allows access to computer applications but without

opening a read and/or write barrier of tab storage means in which access codes are stored. The Tab 26 can also report events generated by its user by pressing buttons on the Tab (col. 7, lines 10-14). As the tab wearer can change of location, it is provided an additional layer of networks addresses in order to keep track of the real address of the mobile unit (tab) and forward packet addresses to the unit appropriately (col. 3, lines 30-35). With several mobile units, it is necessary also to provide an authorization access to a specific mobile unit for security (col. 4, lines 24-29).

As is visible from the above, the operation carried out by the Tab of Want is different from the operations of the portable object set forth in claim 1. That is, Want fails to disclose or suggest the Tab having a control logic module that shapes the password for opening a read and/or write barrier of storage means. In other words, Want fails to disclose or suggest opening a barrier of storage means by a control logic module of the portable object.

Want only discloses an "agent" (application interface), which operates primarily for the benefit of its assigned computer (col. 4, lines 64, 65) in order to allow communications between mobile computer (tab) and its applications. In Want, the specific application for the mobile unit must be authorized by the agent (col. 5, lines 5-7). The agent maintains a list of authorized users or applications (col. 5, lines 16, 17). For each Tab, there is a dedicated process (agent) to handle a variety of tasks exclusively for that specific Tab (col. 8, lines 31-34). Want, however, fails to disclose or suggest checking of a verification word of the portable object in a checking file of a remote specific server, which is not an agent of a computer.

Want only discloses that the Tab can communicate addresses of applications with an identification number in order to allow an agent of a computer station to recognize the personal Tab. Accordingly, the agent is able to control the authorizations of any application to request

communication with the specific mobile unit (the personal Tab). If some applications are personalized for a specific Tab, the agent manages this communication between the Tab and the computer application.

However, Want fails to disclose or suggest the tab having a control module that shapes the password for opening a read and/or write barrier of the storage means. Moreover, Want does not disclose or suggest the tab having a control logic module that connects to the storage means that has a read and/or write barrier (to prevent access to specific applications of the computer without authorizations). That is, Want fails to disclose or suggest a barrier that can be opened by a checking that includes two operations. Specifically, Want fails to disclose or suggest the barrier that can be opened only if:

1. A verification word in a readable part of the storage means has been checked, first, in a checking file located in a server remote from the computer station, connected by Internet, for example, to the computer station. In Want, there is no automatic procedure for sending the verification word when the tab object is located within a predetermined zone of the read unit.
2. Second, when the verification word has been found in the checking file of the server, a password from the server is transmitted to the electronic circuit of the portable object in order to open the read and/or write barrier of the storage means.

Want fails to disclose or suggest that an application addresses can be transmitted from the storage means of the portable object to the computer station to open the personalized applications only after these two operations. In short, Want does not disclose or suggest opening a barrier of storage means to obtain an access word for an application via two checking operations, as set forth in claim 1. In other words, Want does not disclose or suggest two password checking

operations to authorize the opening of personal applications *i.e.*, first, by checking the readable word in the checking file of the remote server and second, by checking the password in the logic control module to open the read and/or write barrier of the storage means.

Contrary to the Examiner's allegation, Want clearly fails to disclose or suggest at least operations (a) and (d) set forth in claim 1. That is, Want fails to disclose an automatic connection to the server is established by components of the peripheral read unit for checking the readable word in a list of authorised words.

Furthermore, the Office Action alleges that the disclosure in col. 7, lines 6-9 of Want renders obvious operation (c) set forth in claim 1. That is, the Office Action speculates that since error detection and correction schemes are well known in the art, one of ordinary skill in the art would have known to execute operation (c) (*see* pages 3-4 of the Office Action). Applicant respectfully disagrees. Applicant respectfully submits that one of ordinary skill in the art would not have come up with the features of operation (c) based on the disclosure of Want in col. 7, lines 6-9. Applicant respectfully submits that the rationale provided in the Office Action amounts to a mere speculation and with this rationale any error detection technique could be rendered obvious. Moreover, the Examiner failed to provide any motivation for modifying Want's disclosure to include the allegedly well known technique.

Pinnow fails to cure the deficient disclosure of Want. Pinnow only discloses an apparatus and a method for a system able to remotely validate the identity of a person and his location by having the person wear on his wrist a device that generates a pseudo-random number sent through a phone line to a base computer station distant from the device. The computer station has a program to generate pseudo-random numbers in order to compare the personalized

pseudo-random number sent from the device in order to check the identity of the person. If the device is not worn by the person, it does not operate and does not communicate its identity.

Pinnow, however, fails to disclose or suggest connecting to a determined remote server in order to check if an identification word of the watch is in authorized words of the server, and transmitting a password from the server to a logic control module of the electronic circuit in the portable object for opening a read and/or write barrier of storage means, and only if the read and/or write barrier is opened, having the read unit communicate access codes to obtain access to personalized applications.

Together, the combined teachings of Want and Pinnow would not have (and could not have) led the artisan of ordinary skill to have achieved the subject matter of claim 1. For at least these exemplary reasons, Applicant respectfully requests the Examiner to withdraw this rejection of claim 1 and its dependent claims 4, 5, 7-11, 13-16, 18, and 21.

In addition, the combined teachings of these references fail to disclose or suggest the reading unit as set forth in the dependent claim 18 and the reading unit as set forth in the dependent claim 21. For at least these additional reasons, dependent claims 18 and 21 are patentable over the prior art of record.

Independent claim 23 recites features similar to, although not necessarily coextensive with, the features argued above with respect to claim 1. Therefore, arguments presented with respect to claim 1 are respectfully submitted to apply with equal force here. For at least substantially analogous exemplary reasons, therefore, independent claim 23 is patentable over the combined disclosure of Want and Pinnow.

Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly invited to contact the undersigned attorney at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

/Nataliya Dvorson/

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Nataliya Dvorson
Registration No. 56,616

Date: May 9, 2006

Attorney Docket No.: Q90918